We claim:

1. An access control method, comprising:

receiving a signal indicative of a combination of two or more unique identity attributes, at least one of the unique identity attributes corresponding to a biometric of a person;

comparing the signal to one or more identity patterns; and

controlling access to a restricted item based on results of the comparing step.

2. The method of claim 1, wherein the restricted item is an area subject to restricted access.

3. The method of claim 1, wherein the restricted item is a system subject to restricted access.

4. The method of claim 1, wherein the controlling step includes:

granting access to the restricted item if there is a match in the comparing step.

5. The method of claim 1, wherein another one of the unique identity attributes is a predetermined distortion pattern, said signal indicative of a distortion of the biometric using the predetermined distortion pattern.

6. The method of claim 1, wherein the predetermined distortion pattern includes a non-linear distortion pattern.

7. The method of claim 1, wherein another one of the unique identity attributes is another biometric of the person, said signal indicative of a combination of the two biometrics.

8. The method of claim 1, wherein the biometric is one of an eye pattern, fingerprint, palm print, voice, handwriting sample, face, and DNA sample.

9. The method of claim 1, wherein said one or more identity patterns are stored in a database.

10. The method of claim 1, wherein said one or more identity patterns are stored in a memory chip.

11. The method of claim 1, wherein the controlling step includes:

denying access to the restricted item if no match occurs in the comparing step.

12. The method of claim 5, further comprising:

generating the identity patterns by distorting biometrics of a respectively plurality of persons using the distortion pattern.

13. The method of claim 12, further comprising:

defining new access requirements by changing at least one of the unique identity attributes.

14. The method of claim 13, wherein the defining step includes:

changing said at least one of the unique identity attributes to a new biometric.

15. The method of claim 13, wherein the defining step includes:

changing the distortion pattern to a new distortion pattern.

16. The method of claim 15, wherein the changing step includes:

generating a new signal for comparison to one or more identity patterns by applying the new distortion pattern to the biometric of the person.

17. The method of claim 13, further comprising:

selecting another distortion pattern to alter access to the restricted item;

generating new identity patterns by distorting the biometrics of said persons using the other distortion pattern; and

controlling access to the restricted item based on the new identity patterns.

18. The method of claim 17, wherein the selecting, generating, and controlling steps are performed in response to a breach in security.

19. The method of claim 18, wherein the breach in security includes theft of distorted biometric information designated in at least one of the identity patterns.

20. The method of claim 13, wherein the defining step includes:

automatically changing at least one of the unique identity attributes on a periodic basis; and

controlling access to the restricted item based on a result of the comparing step performed using said at least one changed unique identity attribute.

21. An access control method, comprising:

detecting a distorted biometric for input into an identification system;

comparing the distorted biometric to one or more distortion patterns; and

controlling access to a restricted item based on results of the comparing step.

22. The method of claim 21, wherein the restricted item is an area subject to restricted access.

23. The method of claim 21, wherein the restricted item is a system subject to restricted access.

24. The method of claim 21, wherein the controlling step includes:

granting access to the restricted item if there is a match in the comparing step.

25. The method of claim 21, wherein the distorted biometric is one of a distorted eye pattern, fingerprint, palm print, voice, handwriting sample, face, and DNA sample.

26. The method of claim 21, wherein the detecting step includes:

detecting the biometric through a non-linear distortion element.

27. The method of claim 21, wherein the controlling step includes:

denying access to the restricted item if no match occurs in the comparing step.

28. A computer-readable medium storing an access control program, comprising:

a first code section which compares a distorted biometric received by an input unit to one or more distortion patterns; and

a second code section which controls access to a restricted item based on results of the comparing step.

29. The medium of claim 28, wherein the restricted item is an area subject to restricted access.

30. The medium of claim 28, wherein the restricted item is a system subject to restricted access.

31. The medium of claim 28, wherein the second code section causes a processor to grant access to the restricted item if there is a match in the comparing step.

32. The medium of claim 28, wherein the distorted biometric is one of a distorted eye pattern, fingerprint, palm print, voice, handwriting sample, face, and DNA sample.

33. The medium of claim 28, wherein the distorted biometric includes a non-linear distortion pattern.

34. An access control system, comprising:

a receiver which receives a signal indicative of a combination of two or more unique identity attributes, at least one of the unique identity attributes corresponding to a biometric of a person; and

a processor which compares the signal to one or more identity patterns and controls access to a restricted item based on results of said comparison.

35. The system of claim 34, wherein the restricted item is an areas which is subject to restricted access.

36. The system of claim 34, wherein the restricted item is a system which is subject to restricted access.

37. The system of claim 34, wherein another one of the unique identity attributes is a predetermined distortion pattern, said signal indicative of a distortion of the biometric using the distortion pattern.

38. The system of claim 37, wherein the distortion pattern is a non-linear distortion pattern.

39. The system of claim 34, wherein another one of the unique identity attirbutes is another biometric of the person, said signal indicative of a combination of the two biometrics.

40. The system of claim 34, wherein the biometric is one of an eye pattern, a fingerprint, a palm print, a voice, a handwriting sample, a face, and a DNA sample.

41. The system of claim 34, further comprising:

a database for storing said one or more identity patterns.

42. The system of claim 34, further comprising:

a memory chip which stores said one or more identity patterns.

43. The system of claim 34, wherein the processor grants access if a match occurs in the comparing step.

45. The system of claim 34, further comprising:

a distortion pattern serving as another one of said unique identity elements.

46. The system of claim 45, wherein the distortion pattern includes a non-linear distortion pattern.

47. The system of claim 45, wherein said signal is indicative of distortion of the biometric using the distortion pattern.

48. The system of claim 47, wherein the identity patterns include biometrics of a respectively plurality of persons which have been distorted using the distortion pattern.

49. The system of claim 34, further comprising:

a storage unit which stores the identity patterns.

50. The system of claim 49, wherein the storage unit stores new identity patterns, said new identity patterns formed by distorting the biometrics of said persons using a new distortion pattern.

51. The system of claim 50, wherein the new identity patterns are stored in response to a breach in security.

52. An access control system, comprising:

a receiver which receives a biometric modified by a predetermined distortion pattern; and

a processor which compares the distorted biometric to one or more identity patterns and controls access to a restricted item based on results of said comparison.

53. An access control system, comprising:

a receiver which receives a modulated biometric; and

a processor which compares the modulated biometric to one or more identity patterns and controls access to a restricted item based on results of said comparison.

54. An access control system, comprising:

a receiver which receives an encoded biometric; and

a processor which compares the encoded biometric to one or more identity patterns and controls access to a restricted item based on results of said comparison.